

SOIP 01270500  
#4

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

JCS79 U.S. PTO  
09/770397  
01/29/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
in this Office.

出 願 年 月 日  
Date of Application:

2000年 2月 3日

願 番 号  
Application Number:

特願2000-032699

願 人  
Applicant(s):

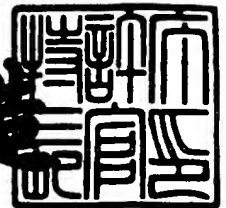
ソニー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年12月 8日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出願番号 出願特2000-3102203

【書類名】 特許願

【整理番号】 9900738506

【提出日】 平成12年 2月 3日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 G11B 20/12

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 千秋 進

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100067736

【弁理士】

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【弁理士】

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【弁理士】

【氏名又は名称】 伊賀 誠司

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ記録方法及び装置、データ再生方法及び装置、並びにデータ記録再生システム

【特許請求の範囲】

【請求項 1】 記録媒体にデジタルデータを記録するデータ記録方法において、

上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成し、

上記デジタルデータのデータ識別情報及びデータ制御情報を上記記録識別情報を用いて暗号化し、

少なくともこの暗号化されて得られた暗号化データと上記記録識別情報とを上記記録媒体に記録すること

を特徴とするデータ記録方法。

【請求項 2】 上記デジタルデータは上記データ識別情報により暗号化されており、この暗号化されたデジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体に記録することを特徴とする請求項 1 記載のデータ記録方法。

【請求項 3】 上記データ制御情報には、上記デジタルデータのコピー制御情報が含まれていることを特徴とする請求項 1 記載のデータ記録方法。

【請求項 4】 上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報を、上記記録媒体に固有の記録媒体識別情報を用いて暗号化し、上記記録媒体に記録することを特徴とする請求項 1 記載のデータ記録方法。

【請求項 5】 上記データ識別情報及びデータ制御情報の暗号化を行うデータ処理部と上記記録媒体にデータを記録するデータ記録部とが分離して設けられ、上記データ記録部で上記記録識別情報を生成すると共に、この生成された記録識別情報を暗号化して上記データ処理部に送ることを特徴とする請求項 1 記載のデータ記録方法。

【請求項 6】 記録媒体にデジタルデータを記録するデータ記録装置において、

上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成する手段

と、

上記デジタルデータのデータ識別情報及びデータ制御情報を上記記録識別情報を用いて暗号化する手段と、

少なくともこの暗号化されて得られた暗号化データと上記記録識別情報とを上記記録媒体に記録する手段と

を有して成ることを特徴とするデータ記録装置。

【請求項 7】 上記デジタルデータは上記データ識別情報により暗号化されており、この暗号化されたデジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体に記録することを特徴とする請求項 6 記載のデータ記録装置。

【請求項 8】 上記データ制御情報には、上記デジタルデータのコピー制御情報が含まれていることを特徴とする請求項 6 記載のデータ記録装置。

【請求項 9】 上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報を、上記記録媒体に固有の記録媒体識別情報を用いて暗号化し、上記記録媒体に記録することを特徴とする請求項 6 記載のデータ記録装置。

【請求項 10】 デジタルデータのデータ識別情報及びデータ制御情報の暗号化を行うデータ処理装置と、このデータ処理装置からの暗号化データを記録媒体に記録するデータ記録再生装置とを有するデータ記録再生システムであって、

上記データ記録再生装置は、上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成する手段と、上記データ処理部からのデータと上記記録識別情報とを上記記録媒体に記録する手段とを有し、

上記データ処理装置は、上記データ記録再生装置からの上記記録識別情報を用いて、上記デジタルデータのデータ識別情報及びデータ制御情報を暗号化し、上記データ記録再生装置に送る

ことを特徴とするデータ記録再生システム。

【請求項 11】 上記デジタルデータは上記データ識別情報により暗号化されており、上記データ記録再生装置は、この暗号化されたデジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体に記録することを特徴とする請求項 10 記載のデータ記録

再生システム。

【請求項 1 2】 上記データ制御情報には、上記デジタルデータのコピー制御情報が含まれていることを特徴とする請求項 1 0 記載のデータ記録再生システム。

【請求項 1 3】 上記データ記録再生装置は、上記データ処理装置からの上記暗号化された上記データ識別情報及びデータ制御情報並びに上記記録識別情報を、上記記録媒体に固有の記録媒体識別情報を用いて暗号化し、上記記録媒体に記録することを特徴とする請求項 1 0 記載のデータ記録再生システム。

【請求項 1 4】 上記データ記録再生装置は、上記記録識別情報を上記データ処理装置に送る際に認証処理を行い、上記データ処理装置が正当であると認証されたとき、上記記録識別情報を暗号化して上記データ処理装置に送ることを特徴とする請求項 1 0 記載のデータ記録再生システム。

【請求項 1 5】 記録媒体にデジタルデータを再生するデータ再生方法において、

上記記録媒体から記録識別情報を用いて暗号化されたデータ識別情報及びデータ制御情報の暗号化データと記録識別情報とを再生し、

上記データ識別情報及びデータ制御情報の暗号化データを上記記録識別情報を用いて復号し、上記データのデータ識別情報及びデータ制御情報を取り出すことを特徴とするデータ再生方法。

【請求項 1 6】 上記デジタルデータは上記データ識別情報により暗号化されて上記記録媒体に記録されており、この暗号化されたデジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体から再生することを特徴とする請求項 1 5 記載のデータ再生方法。

【請求項 1 7】 上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報は、上記記録媒体に固有の記録媒体識別情報を用いて暗号化されて上記記録媒体に記録されており、上記記録媒体から上記固有の記録媒体識別情報を再生し、この再生された上記固有の記録媒体識別情報を用いて、該固有の記録媒体識別情報にて暗号化されたデータを復号し、上記データ識別情報及び

データ制御情報の暗号化データ並びに上記記録識別情報を取り出すことを特徴とする請求項 1 5 記載のデータ再生方法。

【請求項 1 8】 上記データ識別情報及びデータ制御情報の暗号化を行うデータ処理部と上記記録媒体にデータを記録するデータ記録部とが分離して設けられ、上記データ記録部で上記記録識別情報を生成すると共に、この生成された記録識別情報を暗号化して上記データ処理部に送ることを特徴とする請求項 1 5 記載のデータ再生方法。

【請求項 1 9】 記録媒体からデジタルデータを再生するデータ再生装置において、

上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を用いて暗号化された上記デジタルデータのデータ識別情報及びデータ制御情報をの暗号化データと上記記録識別情報とを上記記録媒体から再生する手段と、

上記データ識別情報及びデータ制御情報の暗号化データを上記記録識別情報を用いて復号し、上記データ識別情報及びデータ制御情報を取り出す手段と

を有して成ることを特徴とするデータ再生装置。

【請求項 2 0】 上記デジタルデータは上記データ識別情報により暗号化されて上記記録媒体に記録されており、この暗号化されたデジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体から再生することを特徴とする請求項 1 9 記載のデータ再生装置。

【請求項 2 1】 上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報は、上記記録媒体に固有の記録媒体識別情報を用いて暗号化されて上記記録媒体に記録されており、上記記録媒体から上記固有の記録媒体識別情報を再生し、この再生された上記固有の記録媒体識別情報を用いて、該固有の記録媒体識別情報にて暗号化されたデータを復号し、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報を取り出すことを特徴とする請求項 2 0 記載のデータ再生方法。

【請求項 2 2】 記録媒体からデジタルデータの記録毎にそれぞれ独立の記録識別情報を用いて暗号化されたデータを再生するデータ記録再生装置と、暗号

化されたデータを復号してデジタルデータのデータ識別情報及びデータ制御情報を取り出すデータ処理装置とを有するデータ記録再生システムであって、

上記データ記録再生装置は、上記記録識別情報と上記暗号化されたデータとを上記記録媒体から再生する手段と、これらのデータを上記データ処理装置へ送る手段とを有し、

上記データ処理装置は、上記データ記録再生装置からの上記記録識別情報を用いて上記暗号化されたデータを復号し、上記デジタルデータのデータ識別情報及びデータ制御情報を取り出す

ことを特徴とするデータ記録再生システム。

【請求項 2 3】 上記デジタルデータは上記データ識別情報により暗号化されて上記記録媒体に記録されており、上記データ記録再生装置は、この暗号化されたデジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体から再生することを特徴とする請求項 2 2 記載のデータ記録再生システム。

【請求項 2 4】 上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報は、上記記録媒体に固有の記録媒体識別情報を用いて暗号化されて上記記録媒体に記録されており、上記記録媒体から上記固有の記録媒体識別情報を再生し、この再生された上記固有の記録媒体識別情報を用いて、該固有の記録媒体識別情報にて暗号化されたデータを復号し、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報を取り出すことを特徴とする請求項 2 2 記載のデータ記録再生システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、データ記録方法及び装置、データ再生方法及び装置、並びにデータ記録再生システムに関し、特に、ディスク状記録媒体における不正なディスクコピーを防止するのに好適なデータ記録方法及び装置、データ再生方法及び装置、並びにデータ記録再生システムに関するものである。



## 【 0 0 0 2 】

## 【従来の技術】

ディスク等の記録媒体に記録されたデジタルコンテンツデータ等のデータを他の記録媒体にコピーすることは、著作権の保護等を勘案して、自由にあるいは制限付きで行えたり、完全に禁止される場合があるが、制限付きコピーやコピー禁止の場合には、何らかのデータ保護対策が必要とされる。ここで、上記コンテンツデータには、例えば、音楽、映像、プログラムやテキスト等の著作物が挙げられる。また、ディスク等の記録媒体のコピーを防ぐ方法としては、記録媒体の識別情報（ID）を用いてコンテンツやコンテンツ鍵を暗号化する方法等が提案されている。

## 【 0 0 0 3 】

## 【発明が解決しようとする課題】

ところで、記録すべきコンテンツデータを処理するデータ処理部と、データをディスク等の記録媒体に記録する記録部とが、同一装置内、同一基板上あるいは同一チップ内で一体化されている場合には、お互いのインターフェースから外部にデータが出なければディスクコピーを防止することができる。

## 【 0 0 0 4 】

しかしながら、データ処理部と記録部とが個別の装置に分離されて設けられ、これらの装置間を例えば一般的なインターフェースで接続した場合は、インターフェース間で伝送されるデータを外部に取り出すことができ、データコピーやディスクコピーが可能となる。

## 【 0 0 0 5 】

また、データ処理部と記録部とが同一の装置内、あるいは同一の基板上に設けられている場合でも、データ処理部と記録部との間のデータ線の信号をモニタする等により、データコピーやディスクコピーが行われる可能性も存在する。

## 【 0 0 0 6 】

本発明は、上述の問題点に鑑みてなされたものであって、データ処理部と記録部との間で伝送される信号をモニタされた場合に、データ解読が困難で、データコピーやディスクコピーを防止でき、有効なデータ保護が図れるようなデータ記

録方法及び装置、データ再生方法及び装置、並びにデータ記録再生システムを提供することを目的とする。

【 0 0 0 7 】

【課題を解決するための手段】

上述の課題を解決するために、本発明は、記録媒体にデジタルデータを記録する際に、上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成し、この生成された記録識別情報を用いて上記デジタルデータのデータ識別情報及びデータ制御情報を暗号化し、少なくともこの暗号化されて得られた暗号化データと上記記録識別情報とを上記記録媒体に記録することを特徴とする。

【 0 0 0 8 】

また、本発明にかかるデータ記録再生システムは、上述の課題を解決するために、デジタルデータの暗号化を行うデータ処理装置と、このデータ処理部からの暗号化データを記録媒体に記録するデータ記録再生装置とを有するデータ記録再生システムであって、上記データ記録再生装置は、上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成する手段と、この生成された記録識別情報を用いて暗号化されて得られた暗号化データと上記記録識別情報とを上記記録媒体に記録する手段とを有し、上記データ処理装置は、上記データ記録再生装置からの上記記録識別情報を用いて、上記デジタルデータのデータ識別情報及びデータ制御情報を暗号化し、上記データ記録再生装置に送ることを特徴としている。

【 0 0 0 9 】

ここで、上記デジタルデータはデータ識別情報を用いて暗号化されており、上記デジタルデータのデータ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報を記録媒体に固有の記録媒体識別情報を用いて暗号化し、上記暗号化されたデジタルデータと共に、上記記録媒体に記録することが挙げられる。

【 0 0 1 0 】

上記記録媒体に記録された上記データ識別情報及びデータ制御情報の暗号化データと上記記録識別情報とを読み出して、上記記録識別情報を用いて上記データ

識別情報及びデータ制御情報を復号する。

【 0 0 1 1 】

【発明の実施の形態】

以下、本発明に係るデータ記録方法及び装置、データ再生方法及び装置、並びにデータ記録再生システムの実施の形態について、図面を参照しながら説明する。

【 0 0 1 2 】

図 1 は、本発明の実施の形態となるデータ記録装置の一例となるディスク記録再生装置 1 0 と、このディスク記録再生装置 1 0 に接続される機器の一例としてのパーソナルコンピュータ等のデータ処理装置 1 0 0 の概略構成を示す図である。

【 0 0 1 3 】

この図 1 において、ディスク記録再生装置 1 0 は、着脱可能な追記型光ディスクや、書き換えが可能な光磁気ディスクや相変化型ディスク等の記録媒体であるディスク 3 0 を回転駆動するスピンドルモータ 1 1 と、ディスク 3 0 に対してレーザ光を照射すると共にその戻り光を受光する光学ピックアップ 1 2 と、光学ピックアップ 1 2 のレーザダイオード等のレーザ光源を駆動するレーザドライバ 1 3 と、光学ピックアップ 1 2 から出力された信号を検出する信号検出部 1 4 と、レーザドライバ 1 3 への信号の変調や信号検出部 1 4 からの信号の復調を行う変復調部 1 5 と、データを一時記憶するバッファメモリ 1 6 と、調停部 1 7 と、エラー訂正符号化／復号処理を行う E C C (Error Correction Code) 部 1 8 と、パーソナルコンピュータ等のデータ処理装置 1 0 0 との間でデータを入出力する I / F (インターフェース) 部 1 9 と、データ記録の度毎に異なる記録 I D (識別情報) を生成する記録 I D 生成部 2 0 とを有して構成されている。調停部 1 7 は、バッファメモリ 1 6 と、変復調部 1 5 、 E C C 部 1 8 及び I / F 部 1 9 との間のデータ入出力を調停し、記録 I D 生成部 2 0 からの記録 I D は、 E C C 部 1 8 に送られ、また、外部のデータ処理装置 1 0 0 にも送られる。

【 0 0 1 4 】

スピンドルモータ 1 1 は、図示しないサーボ回路の制御の下に、ディスク 3 0

を一定線速度で、あるいは一定角速度で回転駆動する。

【 0 0 1 5 】

光学ピックアップ12は、ディスク30に対するデータの記録時には、レーザドライバ13により駆動された図示しないレーザ光源からのレーザ光を対物レンズ等の光学系を介してディスク30上に照射して、データを記録する。また、光学ピックアップ12は、ディスク30に記録されているデータの再生時には、図示しないレーザ光源からのレーザ光を光学系を介してディスク30上に照射すると共に、ディスク30の表面で反射回折された戻り光を図示しないフォトダイオード等の光検出素子で受光して電気信号に変換して出力する。

【 0 0 1 6 】

このような光学ピックアップ12によりディスク30に対してデータを記録／再生する際には、受光した戻り光の検出信号に基づいて、トラッキング制御やフォーカス制御を行うことは勿論である。

【 0 0 1 7 】

記録ID生成部20は、記録ファイル（記録内容）に対する固有の識別情報である記録IDを生成する。この記録IDは、データファイル等を記録する毎に更新され、各記録動作に対して固有の識別情報であり、ディスク装置が同じでも、同じディスクに対しても、記録が異なれば異なる記録IDとなる。この記録IDは、例えば乱数発生器等により発生された乱数に基づいて生成すればよい。

【 0 0 1 8 】

記録ID生成部20で生成された記録IDは、そのままデータ処理装置100に送ってもよいが、必要に応じて、暗号化・認証部21により暗号化してデータ処理装置100に送るようにしてもよい。暗号化・認証部21では、上記記録IDに対して暗号化演算 $j()$ を施して、暗号化された記録IDデータをI/F（インターフェース）部19を介してデータ処理装置100に送っている。この暗号化・認証部21は、データ処理再生装置100との間で相互認証を行う機能も有している。

【 0 0 1 9 】

また、ディスク記録再生装置10のディスクID生成部23からは後述するデ

ディスク ID（識別情報）が生成され、これが ECC 部 18 に設けられた暗号化部 24 に送られる。また、暗号化部 24 には、記録 ID 生成部 20 からの記録 ID（識別情報）も送られる。

#### 【0020】

暗号化部 24 は、記録しようとするデータ及び上記記録 ID に対して、上記ディスク ID を用いた鍵によりそれぞれ暗号化処理  $e()$ ,  $f()$  を施し、調停部 17 及びバッファメモリ 16 を介して ECC 部 18 に送り、また、ECC 部 18 から調停部 17 及びバッファメモリ 16 を介して得られた再生データに対して、それぞれ上記ディスク ID を用いた鍵により暗号の復号処理  $e^{-1}()$ ,  $f^{-1}()$  を施す。

#### 【0021】

次に、このようなディスク記録再生装置 10 に接続されるパーソナルコンピュータ等のデータ処理装置 100 は、ディスク記録再生装置 10 との間でデータの入出力を行うための I/F（インターフェース）部 101 と、データの暗号化及び復号（暗号解読）を行う暗号化部 102 と、各種データ処理を行うためのデータ処理部 103 と、外部の認証機関等との間で相互認証等を行うための認証部 104 と、外部との間でデータ識別情報（後述するコンテンツ ID）やデータ制御情報（例えばコピー制限や禁止等の制御情報）の入出力を行うための I/F（インターフェース）部 105 と、I/F 部 101 からの暗号化された上記記録 ID を復号して暗号化部 102 に送る暗号化・認証部 22 とを有している。暗号化・認証部 22 は、ディスク記録再生装置 10 との間での相互認証を行う機能も有している。また、データ処理装置 100 は、コンテンツデータ系として、外部から暗号化されたコンテンツデータを入力する I/F（インターフェース）部 106 と、I/F 部 106 からの暗号化コンテンツデータをコンテンツ ID（データ識別情報）を用いて復号するための復号部 107 とを有しており、コンテンツ ID は、認証部 104 における認証等が正常に行われて正当なユーザであることが確認された場合に、データ処理部 103 から復号部 107 に送られるようになっている。

#### 【0022】

次に、図 1 の構成における動作について、図 2 等も参照しながら説明する。

ディスク記録再生装置 1 0 に接続されるパーソナルコンピュータ等のデータ処理装置 1 0 0 には、認証機関や鍵配送センタ等からのコンテンツ ID 及び制御情報が I / F 部 1 0 5 を介して供給され、また、コンテンツ配送センタやコンテンツプロバイダ等から暗号化されたコンテンツデータが I / F 部 1 0 6 を介して供給されるようになっている。ここで、上記コンテンツデータを  $u$ 、暗号化の鍵となるコンテンツ ID を  $cID$  とし、暗号化処理を  $c()$  とするとき、暗号化コンテンツデータは、 $c(u, cID)$  と表される。また、上記制御情報を  $cIN$  とし、コンテンツ ID  $cID$  及び制御情報  $cIN$  の暗号化処理を  $s()$  とするとき、暗号化されたコンテンツ ID 及び制御情報は、 $s(cID+cIN)$  と表される。

## 【 0 0 2 3 】

図 2 の例では、データ処理装置 1 0 0\_0 からのデータをディスク記録再生装置 1 0\_0 で記録することにより得られたディスク 3 0\_0 を、他のディスク記録再生装置 1 0\_1 で再生する場合を示している。この図 2 のデータ処理装置 1 0 0\_0 には、暗号化されたコンテンツデータ  $c(u_0, cID_0)$  と、暗号化されたコンテンツ ID 及び制御情報  $s(cID_0+cIN_0)$  とが供給されている。

## 【 0 0 2 4 】

データ処理装置 1 0 0 において、例えば認証機関との間で相互認証等を行い、正当であると判断（認証）されたデータ処理装置 1 0 0 には、暗号化されたコンテンツ ID 及び制御情報  $s(cID+cIN)$  が送られる。正当なデータ処理装置 1 0 0 においては、上記  $s(cID+cIN)$  を復号（暗号解読）することができ、暗号化コンテンツの鍵として用いられるコンテンツ ID  $cID$  を得ることができる。

## 【 0 0 2 5 】

すなわち、図 2 の例では、データ処理装置 1 0 0\_0 に供給された暗号化されたコンテンツ ID 及び制御情報  $s(cID_0+cIN_0)$  に復号処理  $s^{-1}()$  を施すことで、元の暗号化前のコンテンツ ID 及び制御情報  $cID_0+cIN_0$  が得られる。配信された暗号化コンテンツデータ  $c(u_0, cID_0)$  は、制御情報  $cIN_0$  により制御される。例えば、コンテンツのコピー回数に制限がある場合に、コンテンツを記録するときには、上記制御情報  $cIN_0$  は例えばデータ処理部 1 0 4 により変更されて  $cIN_1$  となる。この制御情報に応じて、コピー回数が制限されたりコピー禁止とされた

りする。また、上記暗号化コンテンツデータ $c(u\_0, cID\_0)$ は、上記復号されたコンテンツID  $cID\_0$ を用いて復号することにより元の暗号化前のコンテンツデータ $u\_0$ を得ることができる。

## 【 0 0 2 6 】

図2のディスク記録再生装置10\_1では、記録を行う毎に新たな記録ID、例えば $wID\_0$ を発生し、暗号化処理 $j()$ を施してデータ処理装置100\_0に送る。図2のデータ処理装置100\_0においては、ディスク記録再生装置10\_1からの暗号化された記録ID  $j(wID\_0)$ を復号して得られた記録ID  $wID\_0$ を用いて、上記コンテンツIDと変更された制御情報  $cID\_0+cIN\_1$ を暗号化し、暗号化データ $v(cID\_0+cIN\_1, wID\_0)$ を生成し、ディスク記録再生装置10\_1に送っている。上記暗号化コンテンツデータ $c(u\_0, cID\_0)$ は、そのままディスク記録再生装置10\_1に送っている。

## 【 0 0 2 7 】

ディスク記録再生装置10\_1においては、今回の記録に対応して発生された上記記録ID  $wID\_0$ を、図1のディスクID生成部23からのディスクID  $dID\_0$ を用いて暗号化処理 $f()$ を施すことにより、暗号化データ $f(wID\_0, dID\_0)$ を生成し、また上記コンテンツID及び制御情報の暗号化データ $v(cID\_0+cIN\_1, wID\_0)$ に対しては、同じくディスクID  $dID\_0$ を用いて暗号化処理 $e()$ を施すことにより、暗号化データ $e(v(), dID\_0)$ を生成している。なお、この $v()$ は、上記暗号化データ $v(cID\_0+cIN\_1, wID\_0)$ を略記したものである。上記暗号化処理 $f(), e()$ については、上記ディスクID  $dID\_0$ のみならず、必要に応じて、記録単位となるブロック毎の識別情報であるブロックIDを用いるようにしてもよい。これらの暗号化データ $f(wID\_0, dID\_0)$ 及び $v(cID\_0+cIN\_1, wID\_0)$ は、ディスク30\_0にそれぞれ記録され、また、データ処理装置100\_0からの上記暗号化コンテンツデータ $c(u\_0, cID\_0)$ は、そのままディスク30\_0に記録される。なお、上記ディスクID  $dID\_0$ は、ディスクの初期化時やディスクの出荷時、あるいは最初の記録動作時等に、ディスク30\_0上の所定領域に記録される。

## 【 0 0 2 8 】

次に、記録時のディスク記録再生装置10\_0とは異なるディスク記録再生装置

1 0 \_1により上記ディスク 3 0 \_0を再生する場合について説明する。

【 0 0 2 9 】

ディスク記録再生装置 1 0 \_1は、上記ディスク 3 0 \_0より、上記暗号化データ  $e(v(), dID\_0)$  及び  $f(wID\_0, dID\_0)$  を再生し、上記暗号化コンテンツデータ  $c(u\_0, cID\_0)$  を再生し、またディスク 3 0 \_0上の所定領域から上記ディスク ID  $dID\_0$  を再生する。ディスク記録再生装置 1 0 \_1内では、再生された上記暗号化データ  $e(v(), dID\_0)$  及び  $f(wID\_0, dID\_0)$  を、それぞれ上記ディスク ID  $dID\_0$  を用いて復号（暗号解読）することにより、上記コンテンツ ID 及び制御情報の暗号化データ  $v(cID\_0+cIN\_1, wID\_0)$  及び記録 ID  $wID\_0$  を得る。暗号化コンテンツデータ  $v(u\_0, wID\_0)$  については、上記 I / F を介してデータ処理装置 1 0 0 \_1に送り、記録 ID  $wID\_0$  については、暗号化演算  $j()$  を施して、暗号化された記録 ID データ  $j(wID\_0)$  をデータ処理装置 1 0 0 \_1に送る。また、上記暗号化コンテンツデータ  $c(u\_0, cID\_0)$  は、そのままデータ処理装置 1 0 0 \_1に送る。

【 0 0 3 0 】

データ処理装置 1 0 0 \_1では、暗号化された記録 ID データ  $j(wID\_0)$  に対し復号演算  $j^{-1}()$  を施して記録 ID  $wID\_0$  を求め、この記録 ID  $wID\_0$  を用いて、ディスク記録再生装置 1 0 \_1からの暗号化データ  $v(cID\_0+cIN\_1, wID\_0)$  を復号（暗号解読）することにより、上記コンテンツ ID 及び制御情報  $cID\_0+cIN\_1$  を取り出している。このコンテンツ ID  $cID\_0$  を用いて、上記暗号化コンテンツデータ  $v(u\_0, wID\_0)$  を復号し、コンテンツデータ  $u\_0$  を得ることができる。このとき必要に応じて、制御情報  $cIN\_1$  による制限を受けたり、制御情報  $cIN\_1$  自体が変更されるような処理が行われることがある。例えば、別のディスクに再コピーする場合には、制御情報  $cIN\_1$  が  $cID\_2$  に変更される等である。

【 0 0 3 1 】

以上のような実施の形態によれば、ディスク ID  $dID$  と記録 ID  $wID$  とは無関係とすることができるため、ディスク記録再生装置 1 0 とデータ処理装置 1 0 0 との間以外に、ディスク ID  $dID$  や記録 ID  $wID$  が外部に漏洩することを防止できる。また、ディスク記録再生装置 1 0 は、コンテンツ ID 及び制御情報の暗号化演算  $v()$  を知らなくてよい。暗号化演算  $v()$  は、データ処理装置 1 0 0 側の責



任で行い、暗号化演算 $e()$ 、 $f()$  は、ディスク記録再生装置 1 0 側の責任で行うことにより、ディスク記録再生装置 1 0 及びデータ処理装置 1 0 0 の間のインターフェースと、ディスク記録再生装置 1 0 においてディスク 3 0 に対するデータの記録再生とについての各セキュリティを独立させることができる。

#### 【 0 0 3 2 】

次に、図 3 は、上述したような記録 ID を用いた暗号化を施すことによりディスクコピー防止することを説明するための図である。

#### 【 0 0 3 3 】

この図 3 において、データ処理装置 1 0 0 \_0、1 0 0 \_1、及びディスク記録再生装置 1 0 \_0、1 0 \_1 は、上述した図 2 と共に説明した具体例と同様であるため、図中の対応する部分に同じ指示符号を付して説明を省略する。ただし、この図 3 の具体例では、データ記録再生装置 1 0 \_1 からの上記コンテンツ ID 及び制御情報の暗号化データ  $v(cID_0+cIN_1,wID_0)$  及び上記暗号化コンテンツデータ  $v(u_0,wID_0)$  を、他のディスク記録再生装置 1 0 \_2 に送って、他のディスク 3 0 \_2 に記録するようにしている。

#### 【 0 0 3 4 】

すなわち、ディスク記録再生装置 1 0 \_1 は、ディスク 3 0 \_0 を再生することで上記暗号化データ  $f(wID_0,dID_0)$  及び  $e(v(),dID_0)$  を得、ディスク 3 0 \_0 の所定位置に書き込まれた上記ディスク ID  $dID_0$  を用いて復号（暗号解読）することにより、上記コンテンツ ID 及び制御情報の暗号化データ  $v(cID_0+cIN_1,wID_0)$  及び記録 ID  $wID_0$  を得る。また、ディスク 3 0 \_0 を再生することにより上記暗号化コンテンツデータ  $c()$ 、すなわち、 $c(u_0,cID_0)$  を得る。このディスク記録再生装置 1 0 \_1 から得られた上記暗号化データ  $v(cID_0+cIN_1,wID_0)$  及び暗号化コンテンツデータ  $c()$  を、そのまま他のディスク記録再生装置 1 0 \_2 に送って、他のディスク 3 0 \_2 に記録する。ディスク記録再生装置 1 0 \_2 は、ディスク 3 0 \_2 に対応するディスク ID  $dID_2$  を発生してディスク 3 0 \_2 の所定位置に記録すると共に、データ記録の際に記録 ID  $wID_2$  を発生し、この記録 ID  $wID_2$  と上記暗号化データ  $v(cID_0+cIN_1,wID_0)$  とを、ディスク ID  $dID_2$  を用いた鍵により暗号化し、得られた暗号化データ  $e(v(),dID_2)$  及び  $f(wID_2,dID_2)$  をディ

スク 30\_2 に記録する。

【0035】

このディスク 30\_2 を、ディスク記録再生装置 10\_3 で再生する場合には、上記ディスク記録再生装置 10\_2 に記録された暗号化データ  $e(v(), dID\_2)$  及び  $f(wID\_2, dID\_2)$  が再生されてディスク記録再生装置 10\_3 に送られる。また、ディスク 30\_2 から上記暗号化コンテンツデータ  $c()$  が再生されてディスク記録再生装置 10\_3 に送られる。ディスク記録再生装置 10\_3 では、ディスク 30\_2 の所定位置に記録されたディスク ID  $dID\_2$  を読み取って、このディスク ID  $dID\_2$  を暗号鍵として用いることにより、上記暗号化データ  $e(v(), dID\_2)$  及び  $f(wID\_2, dID\_2)$  の復号（暗号解読）を行う。これにより、上記コピーされた暗号化データ  $v(cID\_0+cIN\_1, wID\_0)$  と、この暗号化データ  $v(cID\_0+cIN\_1, wID\_0)$  をディスク 30\_2 で記録した際の記録 ID  $wID\_2$  が復元され、暗号化データ  $v(cID\_0+cIN\_1, wID\_0)$  はそのまま、記録 ID  $wID\_2$  は暗号化演算  $j()$  が施されて、それぞれデータ処理装置 100\_3 に送られる。データ処理装置 100\_3 では、暗号化された記録 ID  $j(wID\_2)$  に対して復号演算  $j^{-1}()$  を施して記録 ID  $wID\_2$  を求め、この記録 ID  $wID\_2$  を用いてディスク記録再生装置 10\_3 からの暗号化データ  $v(cID\_0+cIN\_1, wID\_0)$  を復号（暗号解読）しようとするが、暗号化データ  $v(cID\_0+cIN\_1, wID\_0)$  は記録 ID  $wID\_0$  を鍵として用いて暗号化されたものであるため、暗号化データ  $v(cID\_0+cIN\_1, wID\_0)$  を復号して元のデータ、すなわちコンテンツ ID 及び制御情報のデータ  $cID\_0+cIN\_1$  を得ることができない。

【0036】

すなわち、データ処理装置 100\_3 においては、記録 ID  $wID\_2$  が返されたが、暗号化データ  $v(cID\_0+cIN\_1, wID\_0)$  は記録 ID  $wID\_0$  により暗号化されており、その矛盾から不正にディスクコピーされたことが分かる。また、暗号化データ  $v(cID\_0+cIN\_1, wID\_0)$  は記録 ID  $wID\_2$  では復号されないため、元のコンテンツ ID 及び制御情報のデータ  $cID\_0+cIN\_1$  を得ることはできない。

【0037】

なお、上記ディスクコピーの際に、元の記録を行ったディスク記録再生装置 10\_0 を用いて、ディスク記録再生装置 10\_1 からの再生データをそのまま記録す

ることも考えられるが、記録（コピー）の際に新たな記録IDが生成され、この記録IDは上記元の記録時の記録ID  $wID_0$ とは異なるものとなり、この場合も復号が行えないことになる。

## 【 0 0 3 8 】

次に、図4は、上記記録IDを暗号化せずにディスク記録再生装置10から対応するデータ処理装置100に送る場合を示している。これ以外は、上記図2と同様であるため、対応する部分に同じ指示符号を付して説明を省略する。

## 【 0 0 3 9 】

次に、図5は、ディスク記録再生装置10とデータ処理装置100との間で、上記記録IDのみならず、コンテンツID及び制御情報の暗号化データ $v(cID_0+cIN_1, wID_0)$ についても暗号化を施して伝送する場合の例を示している。

## 【 0 0 4 0 】

すなわち、記録の際には、ディスク記録再生装置10\_1で発生された記録ID  $wID_0$ に暗号化処理 $j()$ を施して得られた暗号化データ $j(wID_0)$ をデータ処理装置100\_0に送り、データ処理装置100\_0では、この暗号化データ $j(wID_0)$ を復号して得られた記録ID  $wID_0$ を用いて、上記コンテンツIDと制御情報のデータ  $cID_0+cIN_1$ を暗号化し、暗号化データ $v(cID_0+cIN_1, wID_0)$ を生成し、さらにこの暗号化データ $v(cID_0+cIN_1, wID_0)$ に対して暗号化処理 $j()$ を施して、ディスク記録再生装置10\_1に送っている。

## 【 0 0 4 1 】

また、再生時には、ディスク記録再生装置10\_1は、ディスク30\_0を再生して得られた上記暗号化データ $e(v(), dID_0)$ 及び $f(wID_0, dID_0)$ を、同じくディスク30\_0から再生されたディスクID  $dID_0$ を用いて復号することにより、上記記録ID  $wID_0$ 及び暗号化データ $v(cID_0+cIN_1, wID_0)$ を求め、これらのデータ  $wID_0$ 及び $v(cID_0+cIN_1, wID_0)$ に対して、それぞれ暗号化処理 $j()$ を施し、得られた暗号化データ $j(wID_0)$ 及び $j(v())$ をデータ処理装置100\_0に送っている。データ処理装置100\_0では、これらの暗号化データ $j(wID_0)$ 及び $j(v())$ に対して復号処理 $j^{-1}()$ を施して、 $wID_0$ 及び $v(cID_0+cIN_1, wID_0)$ を得ている。

## 【 0 0 4 2 】

この図 5 の例における他の構成及び動作は、上述した図 2 の例と同様であるため、対応する部分に同じ指示符号を付して説明を省略する。

## 【 0 0 4 3 】

なお、本発明は、上述した実施の形態のみに限定されるものではなく、例えば上記実施の形態では、データ処理装置とディスク記録再生装置とを個別の装置として説明したが、同一筐体内の別基板、あるいは同一基板上の別回路部としたデータ処理部とデータ記録再生部の場合にも適用できる。また、記録媒体は、ディスク状記録媒体に限定されず、カード状やテープ状の記録媒体等にも適用できる。また、ユーザデータとしては、暗号化されていない平文のデータを用いてもよいが、既に他の暗号鍵により暗号化されているデータを用いてもよい。さらに、上記記録 ID のみならず、ディスク等の記録媒体毎に固有の記録媒体 ID（ディスク ID 等）や、符号化単位あるいは記録単位となるブロック（セクタ、フレーム等）毎に異なるブロック ID を用いるようにしてもよく、この場合、これらの記録 ID、ディスク ID、ブロック ID を生成するための乱数発生器等を共通化するようにしてもよい。この他、本発明の要旨を逸脱しない範囲において種々の変更が可能であることは勿論である。

## 【 0 0 4 4 】

## 【発明の効果】

本発明によれば、デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成し、この生成された記録識別情報を用いて、上記デジタルデータのデータ識別情報及びデータ制御情報を暗号化し、少なくともこの暗号化されて得られた暗号化データと記録識別情報とを記録媒体に記録することにより、記録毎に固有の記録識別情報を用いた暗号化が施されるため、記録媒体からの再生データをそのままコピーしても、データ識別情報の解読（暗号化の復号）が行えず、コピー防止が有効に行える。

## 【 0 0 4 5 】

ここで、上記デジタルデータは上記データ識別情報を用いて暗号化されており、該データ識別情報が復号できない限り、暗号化コンテンツデータの復号が行

えない。

【0046】

また、上記デジタルデータの暗号化を行うデータ処理部と上記記録媒体にデータを記録するデータ記録部とを分離して設けた場合に、データ処理部とデータ記録部との間のデータをモニタされても、データ識別情報の解読が行えず、不正コピーの防止が有効に行える。

【図面の簡単な説明】

【図1】

本発明の実施の形態が適用されるディスク記録再生装置及びデータ処理装置の概略構成を示すブロック図である。

【図2】

暗号化データを記録したディスクを他のディスク記録再生装置で再生する場合を説明するための図である。

【図3】

暗号化データを記録したディスクをコピーしたディスクを再生する場合の一例を説明するための図である。

【図4】

記録識別情報をデータを暗号化しないで伝送する場合を説明するための図である。

【図5】

記録識別情報を暗号化してディスク記録再生装置からデータ処理装置に伝送すると共に暗号化されたデータ識別情報及びデータ制御情報を暗号化してデータ処理装置からディスク記録再生装置に伝送する場合を説明するための図である。

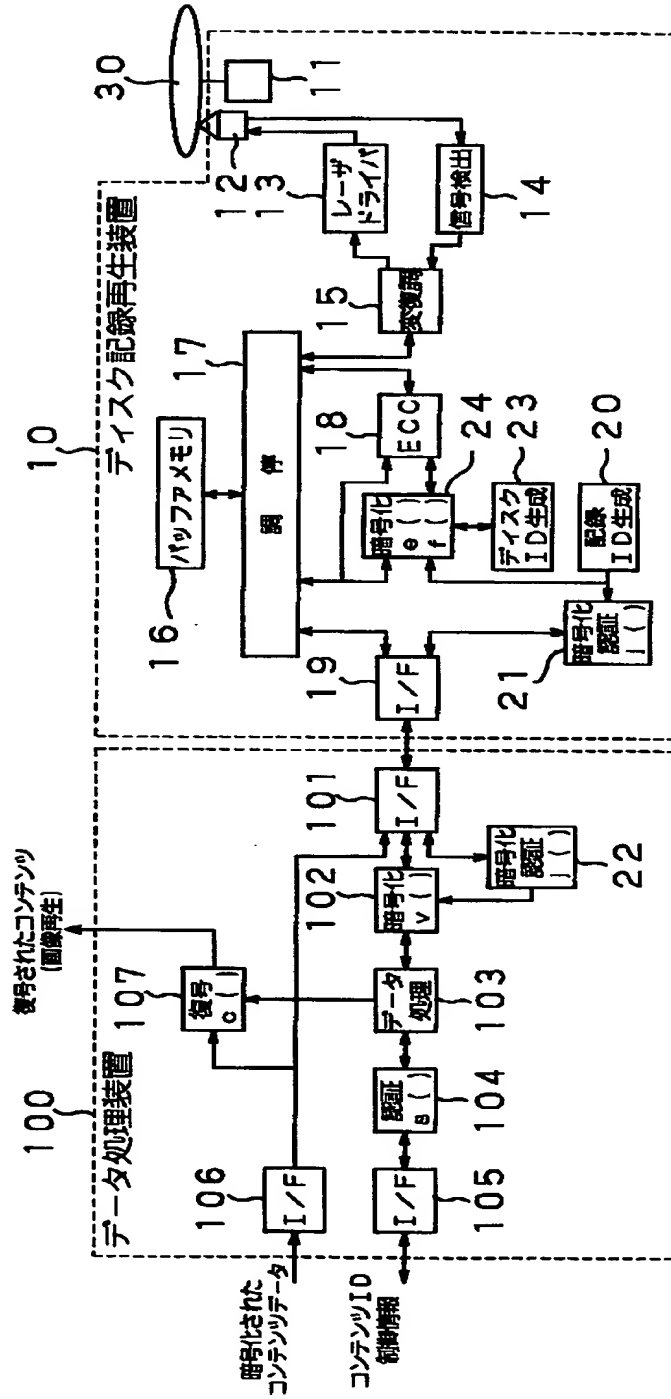
【符号の説明】

10 ディスク記録再生装置、 15 変復調部、 16 バッファメモリ、  
17 調停部、 18 ECC部、 19, 101, 105, 106 I/F  
(インターフェース)部、 20 記録ID生成部、 21, 22 暗号化・認  
証部、 24, 102 暗号化部、 100 データ処理装置、 103 デー  
タ処理部、 107 復号部

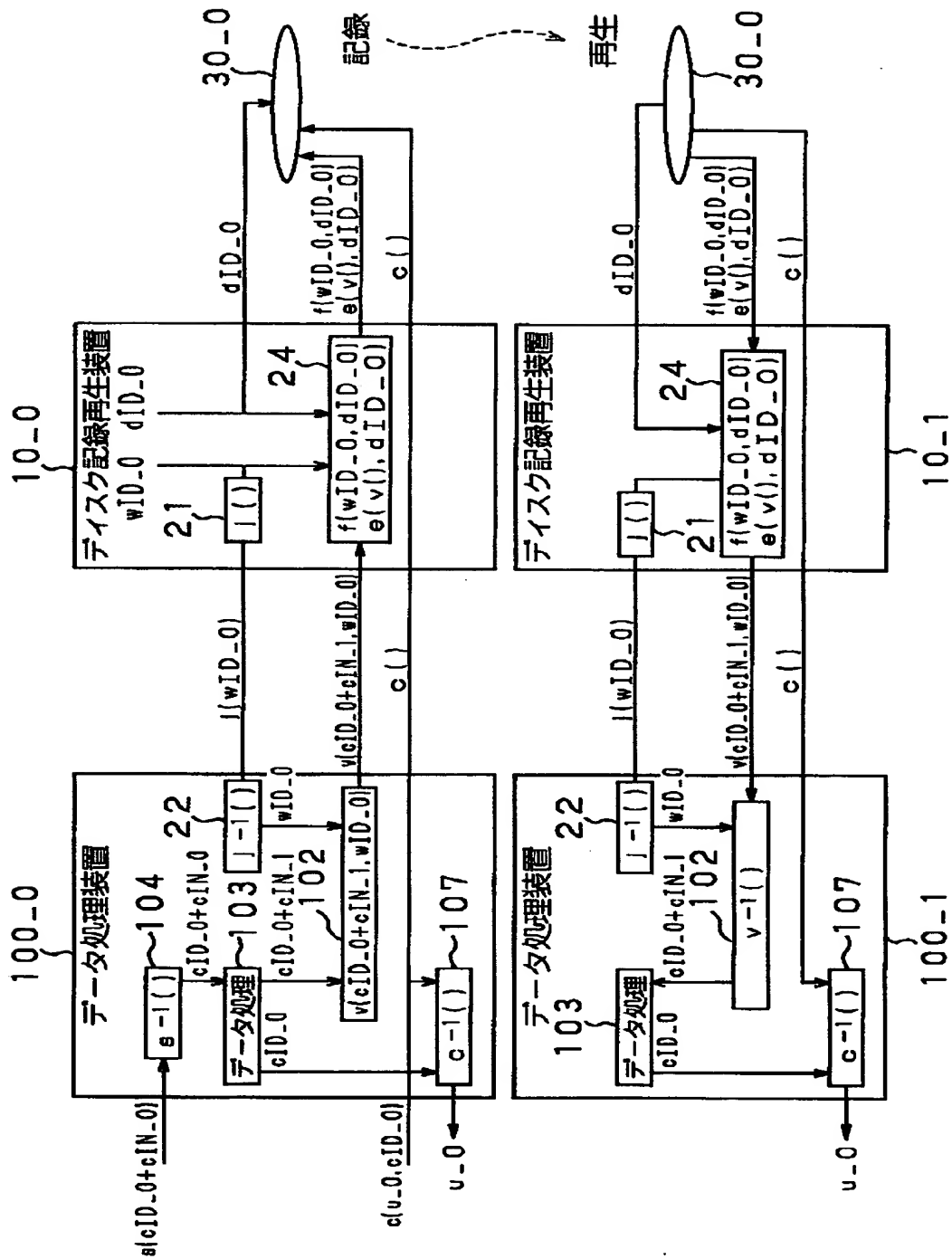
【書類名】

図面

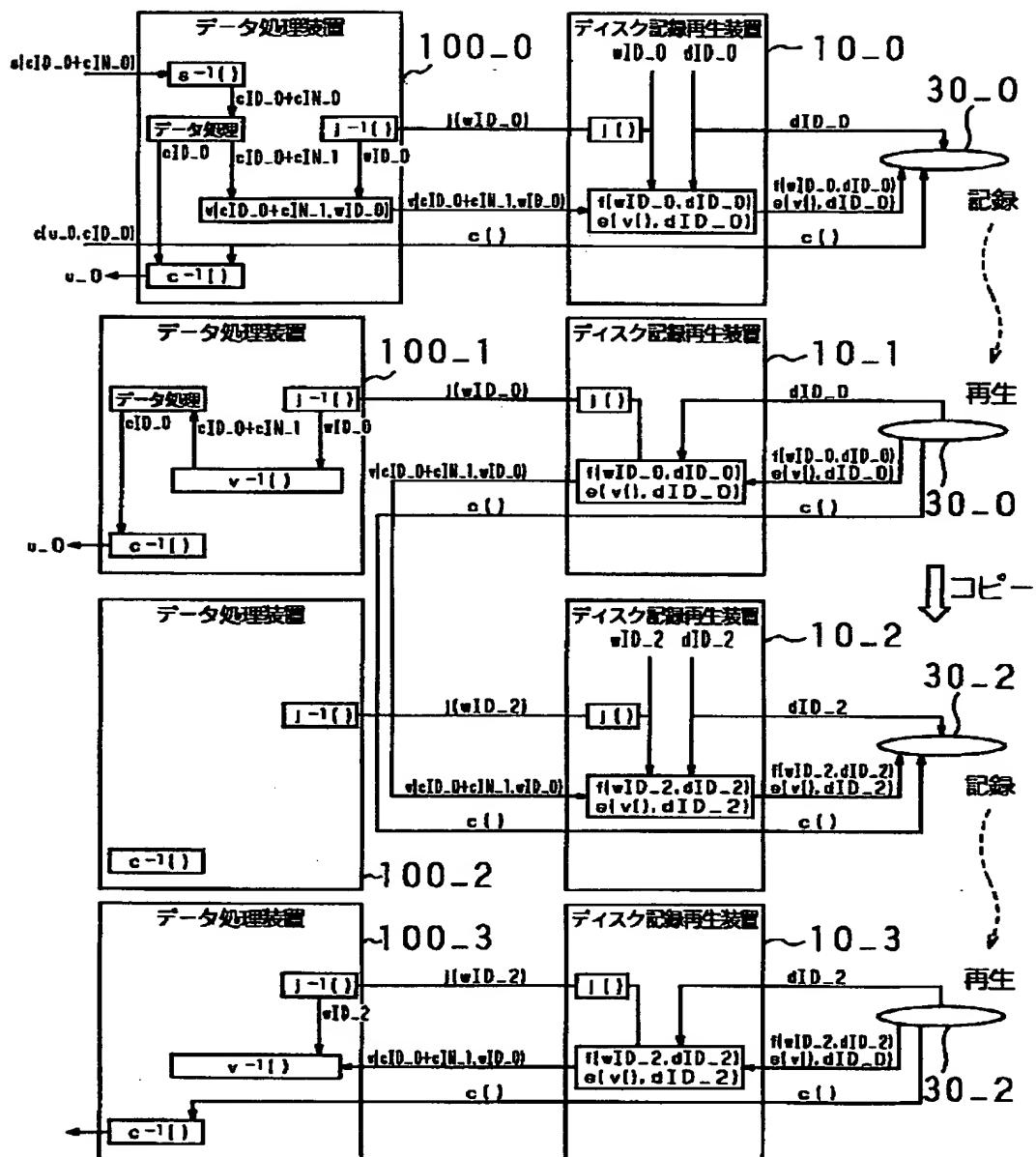
【図 1】



【図 2】

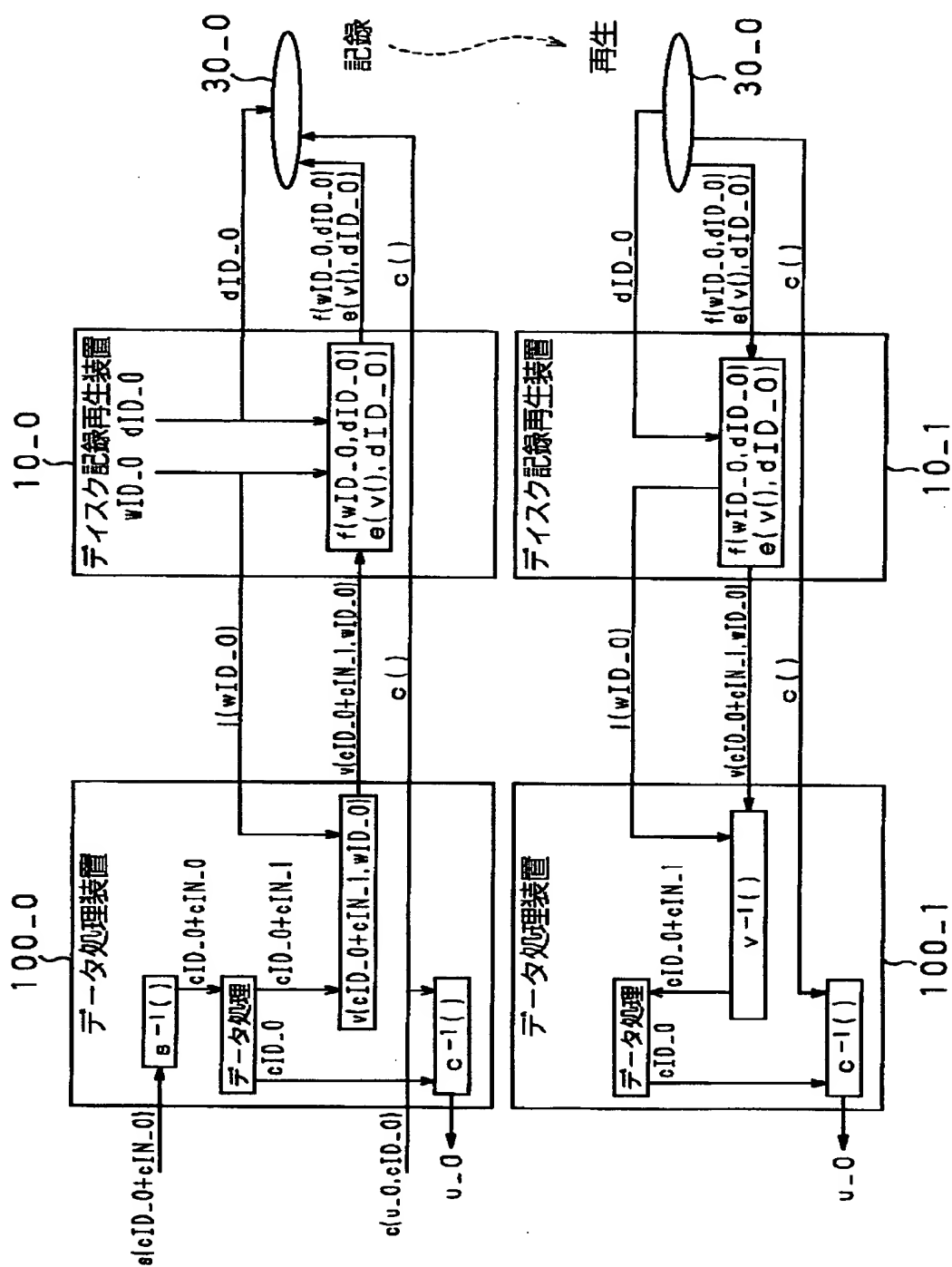


【図 3】

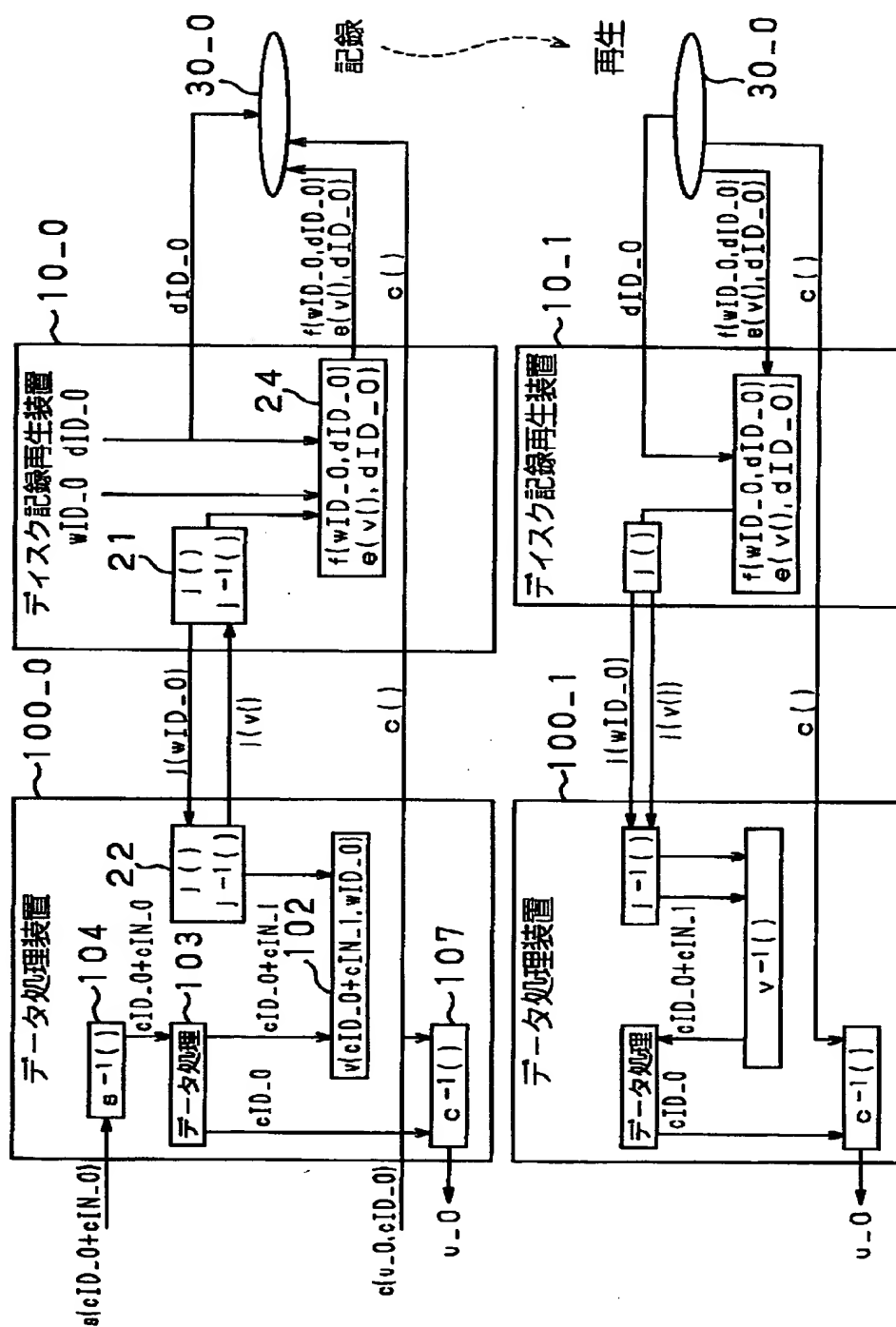




【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 データ処理装置とディスク記録再生装置との間で伝送される信号がモニタされても暗号化されたコンテンツデータのコピー保護が有効に行われるようにする。

【解決手段】 ディスク記録再生装置 1 0 の記録 I D 生成部 2 0 にて記録毎に固有の記録 I D を生成し、この記録 I D をデータ処理装置 1 0 0 の暗号化部 1 0 2 に送って、暗号化コンテンツデータの鍵情報となるコンテンツ I D 及びコピー禁止や制限等を行うためのデータ制御情報を、記録 I D による暗号化の鍵を用いて暗号化する。暗号化されたデータは、I / F 1 0 1、1 9 を介してディスク記録再生装置 1 0 の暗号化部 2 4 に送られ、記録 I D と共に、ディスク I D を用いた暗号化の鍵により暗号化され、ディスク 3 0 に記録される。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社